## **BEST AVAILABLE COPY**



Europäisches Patentamt

**European Patent Office** 

Office européen des brevets



(11)

EP 0 719 045 A2

(12)

### EUROPEAN PATENT APPLICATION

(43) Date of publication: 26.06.1996 Bulletin 1996/26

(51) Int. Cl.6: H04N 7/167

(21) Application number: 95119605.4

(22) Date of filing: 13.12.1995,

(84) Designated Contracting States: DE FR GB

(30) Priority: 13.12.1994 JP 309292/94

(71) Applicant: MITSUBISHI CORPORATION Chiyoda-ku-Tokyo 100 (JP)

(72) Inventor: Saito, Makato Tama-shi, Tokyo (JP)

SOURCE MEDICAGE ARE SEEN. HAV (74) Representative: Neidl-Stippler, Cornelia, Dr. Rauchstrasse 2 1105 12 Per 1 Es D-81679 München (DE)

#### (54)Crypt key system for broadcast programmes

The invention relates to a crypt key system applicable to a television system, a database system or an electronic commercial transaction system or the like. This system consists of a broadcasting station 11, a database 12, a receiving apparatus 14, a data communication apparatus 15 and a user terminal 18. As a crypt key system, a secret-key cryptosystem, a public-key cryptosystem, and a digital signature system are used. The keys used in the system are either encrypted or remain uncrypted to be supplied by broadcasting. The present invention is effective in the prevention of an unjustified use of the database system, managing copyrights,; and in a pay-per-view system and a video-ondemand system. Further, the present invention is effective in realizing an electronic market which uses an electronic data information system.

2 - CAM - 1 /

narya carro int

#### Description

Background of the Invention

#### Field of the Invention

The present invention relates to a crypt key system --that is used in a commercial trade on the like which uses and a television system, a database system or an electronic Fig. 1 or 1 or 1 of 1945 ording anti-

#### Prior Art

In information oriented society of today, in addition to a normal terrestrial broadcasting, satellite broadcasts 115 ing which is referred to as a broadcasting satellites (BS): 15 and communication satellites (CS) or cable TV-broad2 casting which is referred to as CATV (cable television): using coaxial cables or optical cables is getting preva-Philosopon (No. 6 -70748).

In a satellite broadcasting or CATV broadcasting which distributes several tens of channels at the same time, scrambled channels of such as films, sport events@6 and music which cannot be viewed through a compre-inal. hensive contracts are provided in addition to unscrambled general channels. In order to view these channels are it is necessary to subscribe to descramble the channels; 🚿 however, normal subscription period is about one-month unit, and it is impossible to view through temporary contracts:555 a generalization district that it is entitled good so

The inventor of the present invention proposed in the seal. Japanese Patent Application Laid-Open No. 6-46419 3111 and the Japanese Patent Application Laid-Open No.6 141004 a system in which users obtain a viewing permit. 9 7 key from a charging center via a communication line and 2 35 charged, and descrambles programs scrambled each bye respectively different scramble pattern, using the viewing permittkey to view the programs; proposed in the Japa-\*\*\*: nese Patent Application Laid-Open No. 6-132916 an Oct. apparatus' for the operation. Of a Thiorest your society 40

In these system and apparatus, those who wish to 10 4 use ascrambled aprograms arequestrator wiswingsto the percharging center via a communication (line-by easing as 3 communication apparatus. The charging center transmits the viewing permit key to the communication apparate ratus corresponding to the request for viewing while better charging and collecting a fee. who shade in the col

Users, on receiving the viewing permit key with the communication apparatus, transmits the viewing permit \* ... key via direct means connecting the communication 50 apparatus and the receiving apparatus on via indirectors means such as flexible disks or the like. The receiving apparatus to which the viewing permit key is transmitted descrambles the programs with the viewing permit key 🤲 and then, the users use the programs.

Japanese Patent Application Laid-Open No. 6-3 132916 describes a system and an apparatus for sell and rent of a tape or a disk on which a plurality of data scrambled with a different scramble pattern respectively are

### recorded to supply the viewing permit key with IC cards or the like and use a specific data.

> In addition, in these days of information- oriented society, a database system has been propagated for acti mutually, using data which are kept independently by its each computer by constituting a computer communication network by LAN (local area network); WAN (wide:: area network), and Inter-Net system mutually connecting: 300 these networks. doc 医乳腺 医多尿 经基础债金

> In the meantime, attechnology has been developed ..... for reducing the information amount by compressing asset television moving picture signal which could not be digitized because of a huge amount of information as a result 3:45 of digitization, to enable practical digitalization. So far, 49.5 H.261 standard for video conference, JPEG (joint photographic image coding experts group) standard for static pictures, MPEG 1 (moving picture image coding experts group (1) standard for storing pictures and MPEG:2/cor+ 118 responding to the present telecast and the high-definied year tion telecast from the television broadcasting mare up. prepared.

> The digitization technology using these picture compression technology is used for the television broadcasting or the video picture recording. In addition, even television moving picture data which could not be dealt and a with before can be dealt with now. Then, the "multimedia was system" which deals with various data dealt with by the avenue computer and the digitized television moving picture data: 9.89 has been focused as a future technology.

This multimedia system is also incorporated in the data communication and can be used as one data on the database. 16-47 1 37 15 Ca

While the scope of usage of the database is expanded, the method for charging for the data usage on the database; and the method for dealing with copy-1.6.4 right problems generated by copying transmitting other and than direct usage of data, and also the secondary exploitation right problem generated as a result of data edition ( . . . have become important problems. It HETP TIRETINGS

To safely deal with charging and copyrights process and copyrights process and copyrights process are also as a second copyright of the control of the copyright of the copyrigh it is required that the data cannot be used by users other we than authorized users, and data encryption is the best means for it. THE THOMS

In addition, an electronic market system has been investigated for converting information in various kinds 3.3 of transaction which has been carried out by paper documents so far, into an electronic data to execute electronic transaction by susing the electronic data interchange for transmitting and receiving data by the data communication technology. In addition, an investigation is also made on the possibility of carrying out an 32. electronical settlement on the electronic commercial transaction system in the interest of the system of of

In the commercial transactions, the reliability on the transaction details is required and the security in the settlement is required. Consequently, in the electronic commercial transaction system and electronic settlement. 3 systems in which such reliability and security are

3 .....

10

20

7...

demanded, it is required that the data is encrypted so asset that the data will not be falsified or used unjustifiedly.

In these television system, database system or electronic commercial transaction system or the like; the data and is encrypted and thus a crypt key is required for decrypt- 5: ing the encrypted data to us. And the crypt key must be given to data users; however, the processing is very troublesome because security and reliability are demanded.

In the structure of the present invention, data cryptologyacts an important part. In the beginning, a general explanation:will/be made on the data cryptology. and at

In the data cryptology; the case in which the plaintext >>> data Mais encrypted by using a crypt key: K to obtain a main cryptogram data Cis represented: (2) 189 (3) 1941 (24) 6

stand and the particle of the continuous and the continuous brate left trechasC≟E.(K, M), all dig for the grade to the angewanter of the contract of the contract expense

and the case in which the cryptogram data C is decrypted, and by using the crypt key K to obtain the plaintext data M is represented: 3006. . . . to

r feeligiter i pronis u craisee M=D (K, C) in Bassis am and I call su Johrheit

As a typical method for the data cryptography technology:there are a secret-key cryptosystem and a publickey cryptosystem::The Secret-key cryptosystem is:a :: cryptosystem in which same secret key Ks is commonly #8 used in encryption and decryption . . . 

00 1 7 T. 27 3 ,21 ٠. ٦ 30 serios disastilo Cmks≠Et(Ks, M) de action while the training opens M=D (Ks, Cmks) ය සිදුන්නු ළුජී වී දකුකට නිලා ය

The public- key cryptosystem is a cryptosystem in an which a key for encryption and a key for decryption are 35 used as crypt keys, and the key for encryption is laid open 😁 but the key for decryption is not open. The key for encryption is referred to: as a public-key Kb while the key for decryption is referred to as a private-key Kv. To use this: cryptosystem, an information sender encrypts, the plaintext data M by the pubic-key Kb of a seceiver

tead and all noting one sate of the letter from the sate Cmkb=E (Kb, M), mend and messys someon and these har hors been

and the receiver receives the data and decrypts it by a ; 45 private-key Kv to obtain the plaintext data Marcollin such appoints on the live in a market

நாது நாம்ந்த**M=D.(Kv, Çmkb)**.. ுக்கார் and dispersion ones in the community of the community In this public-key cryptosystem, cryptanalysis is very dif- 50 ficultion programmes for the first back

As an application of the data cryptography technology, digital signature is performed as an electronic data authentication means to ensure the reliability of the data.

The digital signature is used a secret-key or a public- 55 key. Generally, the public-key is used in the digital signature. Per per passion of the · S. 33 W 7'8 "

In the digital signature which is carried out by using:2 the public-key, the signer obtains a digital signature by

encrypting a document m to which the document M is compressed with hash algorithm, using the private-key Ky of the signer:

#### Smkv=E (Kv, m)

and transmits the original document M or the compressed document m and the digital signature Smkv to the receiverals dishormed with a titure year of tage notices and a

The receiver decrypts the digital signature Smkv by. : using the public-key Kb of the signer

m'=D (Kb, Smkv).

withbox as with the relative comes in wife model in When miam is established, it is recognized that the signature is; corrected growant sendings (2015) 19 (34), the North

Assemethod for providing these crypt keys to users; ..... the inventor of the present invention proposed an invention of tion entitled "crypt key system".in the prior Japanese Patent Application No. 6-70643.

in the generally practiced crypt key system, the crypt key is provided only to users while the crypt key is provided to persons other than the users in the crypt key and system of this prior, invention, and address startly places as E Figure shows the structure of the crypt key system (a) proposed in the Japanese; Ratent Application No.: 6- 1-11 70643 jern sind er meturn utdand i med tokkula ut had kattille i m

This system comprises a proadcasting station 1 for way multiplex boadcasting such as BS,GS,iterrestrial broads the casting or FM or the like or data broadcasting, a datasthesis base; 21 a charging center 3, a receiving apparatus; 47 data communication apparatus 5 and a user's terminal 8.50 de

The broadcasting station it and the database 2, and the the database 2 and the charging center 3 are connected) to each other via a communication line such as a dedicated line or the like or flexible disc or the like. The data: base 2 and the data communication apparatus 5 are connected by a communication line 7 such as a commu-men nication fine on CATY/line of plant in the C The broadcasting station 1 and the receiving apparatus 4 are connected with the broadcasting radio wave 6. The receiving apparatus 4 and the user terminal apparatus and 8, and the data communication apparatus 5 and the user smo terminal 8 are connected with a direct means such as arecconnection cable on an indirect means such as a flexible discalidad granado not tabular actividad productiva actividad

In Fig. 1, what is shown with a solid-line is a path of a solid-line is a path of information, which is not encrypted. What is shown with a broken line is a path of data which is encrypted and account

In this system, the database 2 preliminarily supplies a permit key Kp (hereinafter referred to as a "permit key") >: including the crypt key Kd which is different from one data to another to the breadcasting station 1. The permit key Kp is explained in such a manner that the permit key Kp constitutes the crypt, key. Kd only, for better understanding. Fact 3. Call 135 34 .847.726 .

In some cases, the crypt key Kd is supplied without 🕆 being encrypted and in other cases, it is encrypted by: ... using the common crypt key K0. CONSTRUCTION OF STATE imbros in A

#### Ckdk0=E (K0, Kd),

and is supplied as an encrypted crypt key Ckdk0340.00 II

In the case where the crypt key Kd is encrypted and supplied, a common crypt key K0 for decrypting the sencrypted crypt key Ckdk0 is supplied to usersoffhis common crypt key K0 is supplied when users register with the database; or it is supplied to the users together with the encrypted data Cmkd when the encrypted data Cmkd is transmitted?

(a) In the case where the crypt key is not encrypted? Of the case where the crypt key is not encrypted? Of the case where the crypt key is not encrypted?

The receiving apparatus 4 supplies the received crypt key Kd to the user terminal 8 so that the user terminal 8 stores the received crypt key Kd in a recording medium such as a semiconductor memory, a flexible 20 disc, a hard disc or the like 16 and 17 series 20 and

The users who wish to use the data request for the 1/15 use of the data M to the database 2 via the committing at 1 or tion line 7 by using the data communication apparatus 5.000

The database 2 which has received the request for 1925 use of the data M encrypts the data M by the crypt key. For Kd which is a permit key Kp. For No. 19 For the columnous was a goldenous or the form. The form of the Property of the Columnous Co

and transmits the encrypted data Cmkd to the data complete munication apparatus 5 of users via the communication along softward the communication and charges with the charging center 3. The data seems to be seen and charges with the charging center 3.

The data communication apparatus 5 supplies the received encrypted data Cmkd to the disenterminal 8 most while the disenterminal 8 decrypts the encrypted data out Cmkd by the crypt key Kd which is stored in the recording medium.

M=D (Kd, Omkd)and den ji dhe na dur Saud with i di neevileu agran who a be yiliahabbari

(b) In the case where the crypt key is energet and thes a common crypt key is preliminarily distributed to see the common crypt key.

In this crypt key system, when users register to use 45 the database, the common crypt key K0 is supplied to 2 users with the recording medium such as ROM or flexible disc and the supplied common crypt key K0 is stored in the user terminal 8.

The database 2 encrypts the crypt key Kd by using 50 the common crypt key KO St. A the Common cr

and supplies encrypted crypt key Ckdk0 to the broad-9755 casting station 1.

The broadcasting station 1 broadcasts the received encrypted crypt key Ckdk0 supplied from database 2 by a using the radio wave 6.

The receiving apparatus 4 supplies the received encrypted crypt key Ckdk0 to the user terminal 8 which decrypts the encrypted crypt key Ckdk0 in the beginning by the preliminarily stored common crypt key K0

Kd=D (K0, Ckdk0),

and stores the decrypted crypt key Kd in the recording medium such as a semiconductor memory, a flexible disc or a hard disc.

Users who wish to use the data requests for the use of the data M to the database 2 via the communication line 7 by using the data communication apparatus 5.

The database 2 which receives the request for the data usage encrypts the data M which is demanded for segmentations usage encrypts data M by the crypt key Kd

en i jaran en jaran e

or confirmation cash

and transmits it to the data communication apparatus 5 % (%) via the communication line 7 and chargess with the 155 charging center 3.

The data communication apparatus 5 supplies the FURD received encrypted data Cmkd to the user terminal 800 48 which decrypts the encrypted data Cmkd by the stored 1988 crypt key Kd State 48 St

M=D (Kd, Cmkd). The parameters tensis

In this crypt key system, the database 2 encrypt the common crypt key K0 by the common crypt key K0

Ckdk0=E (K0, Kd) ফাঠি চাটি জেলিক কিছিলটি ভূট

and supplies it to the broadcasting station 1.1 (1) phon to

The broadcasting station 1 broadcasts the encrypted crypt key Ckdk0 which has been supplied from the database 2 by using the radio wave 6 in the

The receiving apparatus 4 supplies the received encrypted crypt key Ckdk0 to the user terminal 8. The user terminal 8 stores the encrypted crypt key Ckdk0 in recording medium such as a semiconductor memory, a flexible disc, or a hard disc or the like.

Users who wish to use the data request for the use of the data M to the database 2 via the communication line 7 by using the data communication apparatus 500 miles.

The database 2 which receives the request for the data usage encrypts the data M which is demanded for use by the crypt key Kd at 4 and 3 and 4 and 3 and 4 and 3 and 4 and 4

Cmkd=E (Kd, M),

and transmits it to the data communication apparatus 5 via the communication line 7 together with the common crypt key K0 and charges with the charging center 3.

30

40

The data communication apparatus 5 supplies the received encrypted data Cmkd and the common crypt ::: key K0-to the user terminal 8. The user terminal: 8 230 decrypts the encrypted crypt key Ckdk0 which has been and stored in the recording medium by the common crypt key 5 K0

and decrypts the encrypted data Cmkd by the decrypted 10. crypt-key-Kd crass and and a second restriction 1. 化多数 医感觉 1. 1980 April 1. 1

a physical M=D (Kd, Cmkd). Apply are year gardina was the definite agen-

Summary of the Inventions of the second of t

10032, 200, 0760

The present invention provides a concrete structure for applying the invention of the crypt key system described in the previous applications to the television system; the database system or the electronic commercial transaction system or the like.

This system comprises a broadcasting station, a database, a receiving apparatus, a data communication apparatus, and a user terminal. As the crypt key system, secret-key cryptosystem and the public-key cryptosystem are used. In addition, the digital signature is used, and the crypt key is supplied through broadcasting with either encrypted or uncrypted.

The present invention is effective in the prevention from unjustified use or the copyright management in the database system, a pay-per-view system, or a video-ondemand system. Furthermore, the present invention is a useful means in the realization of an electronic market using the electronic data interchange system.

#### 1 miles 1 miles 1 miles Brief Description of the Drawings

ng ninggarage ngang kilang

Alternative and the second of the i viki su ku ili masa na masa Masa na masa n

1 1 1 1 1 1 1 1 1 1 1 1 1 1 Fig. 1 is a structural view of a crypt key system according to the prior applications.

ari nalata . . . . 151 Eig. 2 is a structural view of the crypt key system provided according to a first embodiment of the present inventhis necessarity and enteresting the recording

e AT A feriorited real of the Table Tolke in a Fig. 3 is a structural view of the crypt key system 45 according to a second embodiment of the present rapar in the

ila dalah ketalah salah sa Fig. 4 is a structural view of the crypt key system according to third and fourth embodiments of the 50 present invention.

Figs. 5(a), 5(b) and 5(c) are structural views of fifth ..... embodiment to which the present invention is . ( . . . . applied.

**Embodiments** 

Embodiments of the present invention will be described by using Figs. 2 through 4.

· 77 3

[Embodiment 1], a on the

out godes have all

anadera a transfer ico

A system shown in Fig. 2 is a crypt key system of the embodiment 1 in which the present invention is it. applied to a database system. This system comprises a comprises broadcasting station 11 which either a multiplex broadcasting by of BS, CS; a terrestrial wave television, or FM. broadcasting or the like, or data broadcasting by a digital broadcasting, a database 12 in which various kinds of data including moving picture data is stored, a charging ... center 13, a receiving apparatus 14 for receiving the data , - - > broadcasting offered by the broadcasting station 11, a data communication; apparatus 15 for communicating with the database 12 and the user terminal 18 for using the dataxestical electors in acroupatruly and only on more than

The database 12 and the broadcasting station 11, 5 and the database 12 and the charging center 13 are connected with a direct means connecting with a communication line such as a dedicated line or an indirect means: such as a flexible disc on the like. The database 12 and the data communication apparatus 5 are connected with a communication line 17 such as a communication line. or CATV line or the like. Then, the broadcasting station 11 and the receiving apparatus 14 are connected with a radio wave 16 such as a terrestrial wave television broadcasting, satellite-television broadcasting, CATV broadcasting, FM broadcasting or a satellitedate broadcasting or the like. The receiving apparatus 14 and the user terminal 48, and the data communication apparatus 15 and the user, terminal 18 are connected with a direct means such as a connection cable or an indirect means such as a flexible disc or the like

What is shown with a solid line in Fig. 2 is an are uncrypted data path and what is shown with a broken line is an encrypted data path; (20) 250

Incidentally, data exchange between the database 12 and the broadcasting station 11, and the database 12, and and the charging center 13 are, in principle, carried out with a dedicated line or a flexible disc. In addition, a public line, a broadcasting satellite, a communication satellite or a terrestrial wave broadcasting can be used. In such a case; the data is encrypted.

In this system, the secret-key cryptosystem and the public-key cryptosystem are used. . . . . . चे ची क्वा

The database 12 prepares the public-key Kbd and the private-key Kvd to supply the public-key Kbd to the broadcasting station 11. The broadcasting station 11 which receives the public-key Kbd broadcasts it by a teletext multiplexing broadcasting using scanning lines during the retrace blanking interval period of an arnalog television picture signal, the data broadcasting using a sub audio band of the analog television audio signal, FM multiplex data broadcasting or digital data broadcasting.

Service of the servic

1.24

. 100

Further, in this case, a digital signature of the data-

The data may be supplied without encrypting the menu in which the titles of data which can be used; the content introduction of the data, product catalogs; order 15 forms, blank checks, the copyright information for the 25 convenience of the data usage.

The receiving apparatus 14 which receives the transferred public-key Kbd sends the public-key Kbd to the user terminal 18. The user terminal 18 which 10 receives the transferred public-key Kbd stores the public 10 key Kbd in the recording medium such as a semiconductor memory, a flexible disc, or a hard disc or the like.

Users who select the data which they request for the usage by means of menu or the introduction of contents are request for the use of data M to the database 12 via a communication line 17 by the data communication apparatus. 15.

At this time, the user encrypts the public-key/kbd of the the database 12 by own secret-key Ksu which, has 5.20 received from the database 12.00 colored to be become at the colored to

Including the size of payons against the property of the property

Cksukbd=E (Kbd; Mksu) act pages intom de company of a seguinted a Property of the company of the

and transmits it to the database 124 Contain Contain Contain 225

The database 12 decrypts the encrypted secret-key to Cksukbd of the user by the private-key Kvd (2003) as 198 for 2004 (2004) as 198 for 2004 (2004).

and encrypts the data M which is requested for userby as the decrypted users served by the decrypts of the data of the decrypts of the data of the decrypts of

Cmksu=E<sup>\*</sup>(Ksu, M)assection be entitive to the data communication apparatus:1,5° and

of the user via the communication line 17/2 to the protect the last the user who receives the data Cmksu encrypted to by own secret-key Ksu decrypts the encrypted data. Cmksu-with the user terminal, 18 to the user to the same as at the 40 cmksu-with the user terminal, 18 to the user terminal term

ay the control of the control of the figure of the factor of the control of the

This system is provided with charging center 13. 45 which is incorporated with the database 12. This charge 14 ing center 13 is used when the data is provided with pay basis. In the case where the data is one which is provided with free such as shopping information or the like, this charging center 13 is not used. However, even the data 150 provided with free such as shopping information or the like, the charging center is used in the case where charges are to be settled along with orders.

\$4. 1 A A A A

Fig. 3 shows a crypt key system according to sage embodiment 2 in which the present invention is applied to a video on demand (VOD) system which broadcasts

television programs corresponding to the requests from users.

This system comprises a CATV station 21, a charging center 23, a receiving apparatus 24, a data communication apparatus 25 and a user terminal 28.

The charging center 23 is used when the television program is provided on pay basis but not used when the stelevision program is provided without charges along with advertisement.

In this system, the encrypted television broadcast programs and the crypt key are transmitted with the CATV line 27 which is a single path.

The CATV station 21 and the charging center 23 are connected with a direct means for electrical connection with a communication line such as a dedicated line or the like, or an indirect means such as flexible disc on the like. The CATV station 21 and the receiving apparatus 24, the CATV station 21 and the data communication apparatus 25 are connected with the CATV cable 27. The receiving apparatus 24 and the user terminal 28, the data communication apparatus 25 and the user terminal 28 are connected with a direct means such as a connection cable or an indirect means such as a flexible disc or the like.

What is shown with a solid line in Fig. 3-is an of uncrypted data path and what is shown with a broken similar is an encrypted data path.

Incidentally, the data exchange between the CATV-Station 21 and the charging center 23 is carried out through a dedicated line or a flexible disc in principle. Additionally, the data exchange is also carried out by the means of the communication-line or the broadcasting as satellite, the communication satellite and the terrestrial wave broadcasting. In this case, the data is encrypted.

In this system, the CATV system is treated as one kind of database. As a crypt key method, the secret-key of a cryptosystem and the public-key cryptosystem are adopted.

Users who use this VOD system either registers their day own public-key Kbu with the CATV station 21 in advance, or transmit the public-key Kbu by using the communication apparatus 25 at the time when the request for usage?

The CATV station 21 encrypts the secret-key Kebrosti of the CATV station 21 by the transmitted public-key/Kbul?10 of users

் Cksbkbu=E (Kbu, Ksb) ் கட்சம் டின்ற ஒண்

and transmits it to the data communication apparatus 25 via the CATV line 27

医水杨醇 电电流 化氯基酚 化烷基酚基酚盐

ি এক ১৯১১ চন্দ্ৰীয় কেন্দ্ৰ

The television program M is encrypted by using the secret-key Ksb of the CATV station 21 control and the secret se

Sec. St. Crnksb=E (Ksb, M) 1 2 Pk. 2 Pc 1 bit 13.

and is broadcast to the receiving apparatus 24 via the CATV line 27.

6

ក្រសួទប្រធានជា

 $V'' \subseteq U''$ 

The user decrypts the received encrypted secretkey Cksbkbu of the CATV station 21 by the private-key Kvu of user

Ksb=D (Kvu, Cksbkbu)

and decrypts the encrypted television program Cmksb using the decrypted secret-key Ksb of the decrypted CATV station 21

for use. : )

1 30% 2 65%

In addition, this crypt key system is applicable, if encryption is available, to the television broadcasting other than CATV, audio broadcasting, or data broadcasting. As a method, for transmitting the crypt key from the broadcasting station, the teletext multiplex broadcasting using the scanning lines during the retrace blanking inverval of an analog television ppicture signal, the data broadcasting using an sub audio band of the analog television audio signal, FM multiplex data broadcasting; or digital data broadcasting can be also used.

In addition, this crypt key system can be used when the crypt key is distributed in the data copyright manage ament system which is described in prior Japanese Patent Applications Nos. 6-64889, 6-237673, 6-264199, 6-264201 and 6-269959 proposed by the present inventor.

This crypt key system can be also applied to a case where a recording medium such as a CD-ROM or the: 30 like in which a plurality of informations are encypted with a plurality of different patterns and are recorded, which is described in Japanese Laid-Open Patent Application 85 No. 6-132916, proposed by the present inventor.

These inventions of previous applications are explained hereinbelow: The set in the set of the set

An outline of the data copyright management system described in Japanese Patent Application No. 6-64889 is described as follows.

To control the copyright in the display (including the 1940 process to sound); storage, copy, edit and transfer of digital data in the database system including a real time transmission of a digital picture, any one or a plurality among a program for managing the copyrights a copyright information and a copyright management message 45 are transmitted, when needed, in addition to a permit key for allowing the use of encrypted data corresponding to usage requests from users.

The copyright management message is displayed on a screen and advises or warns to the user in case the data is utilized other than the conditions of user's request or the permission. The copyright management program watches and controls in order that the data is not utilized beyond the conditions of user's request or the permission.

The copyright management program, the copyright information and the copyright management message are This supplied together with a permit key in some cases, or they are supplied together with data in some other cases.

Or, a part of them is supplied together with the permit key, and other part is supplied with the data.

For data, the permit key, the copyright management message, the copyright information and the copyright management program, there are the following three cases: and case where these are transmitted with encrypted, and upon using, the encryption is decrypted, a case where they are transmitted with encrypted and remain in encrypted except being decrypted only when they are displayed, and a case where they are not encypted at all and a case where they are not encypted at all and a case where they are not encypted at all and a case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted at all and case where they are not encypted and cas

An outline of the data copyright management system described in Japanese Patent Application No. 6-237673 is described as follows:

This database copyright management system comprises a database in which uncrypted data is stored? a data supply means of a breadcasting station such as satellite broadcasting station for broadcasting the encrypted data from the database; or of a recording medium such as a CD-ROM where encrypted data from the database is recorded, a communication network, a key control center for controlling a crypt key, and a copyright management center for controlling copyrights of the database. Then, the database utilization program for using the database, the copyrights affirst crypt key and a second crypt key are used.

A first user registers with the key control center in advance for using the database. At that time, the database use program is distributed. This database utilization program includes information on the first user and a program for generating a ctypt key unique to the first user with a predetermined algorithm by using the information.

The data is stored in the database without encrypted, and when it is distributed by broadcast; or through recorded on a recording medium or a communication network, the databis encrypted by the first crypt key to an encrypted data and the store of the

The encrypted datal is stored in recording medium such as a semiconductor memory of the first user terminal, a flexible disc or hard disc, when distributed via broadcasting or communication network; is stayed as is when recorded in a CD-ROM recording medium and distributed, or is stored in the recording medium such as a semiconductor memory of the first user terminal, a flexible disc or a hard disc or the like of the street and the second services.

The first user who uses the data directly from the database requests a key for decrypting and using the encrypted data to the key control center via the communication network. Information concerning the first user is presented at this time: 200

The key control center transfers the information on the first user to the copyright management center while the copyright management center uses information I concerning the first user to generate a crypt key peculiar to the first user by a predetermined algorithm, and the generated first user crypt key is used to encrypt the copyright management program, the first crypt key and the

second crypt key to be transferred to the key control or center.

The copyright management program encrypted by using the crypt key generated by using the information on the first user is peculiar to the first user.

The key control center which receives the encrypted copyright management program transmits to the first user terminal each of the encrypted copyright management program, the first crypt key and the second crypt key via the communication network. Then, the first user 10 stores the received encrypted copyright management program, the first crypt key and second crypt key inca recording medium such as a semiconductor memory, a.z. flexible disc, on a hard discretized as the second crypt.

The first user generates the crypt key peculiar to the first user by using a database utilization program which is distributed in advance and using information on the strict user with a predetermined algorithm. Then, the first user decrypts the encrypted copyright management program, the encrypted first and second crypt keys, and the encrypted data is decrypted by the decrypted first crypt key.

In the case of storing, copying and transferring these decrypted data, it is encrypted by the second crypt key decrypted with the decrypted copyright management 25 program. Then, the encrypted data is stored in the recording medium such as the semiconductor memory of the first user terminal, the flexible disc or the hard disc or the like. When the first user uses the stored encrypted data, it is decrypted by using the second crypt key. Then; 30 this operation is repeated for primary sue of the data?

When the encrypted data is copied on the external memory medium or is transferred to the second user televior minal via the communication network, the first crypt-key and the second crypt key are disued by the copyright wish management program. The first user then, cannot use the encrypted data.

At this time, when the encrypted data is stored in the first user terminal, uncrypted information on the first user to is added to the encrypted data which is stored. If yellong is

In the case where the first user uses the encrypted data gain, the first user obtains the first count he second crypt key from the copyright management center. With the regrant of the first crypt key and the second crypt key, it is confirmed that the second user exists which has 45 received the copy or the transfer of the encrypted data from the first user, and the fact of the second user is recorded on the copyright management center.

The second user who has received the copied or transferred encrypted data requests for the secondary use of the encrypted data to the copyright management center. The second user is not required to register with the key control center preliminary, unlike the first user. At the time of the request for data use, with the presentation of the information of the first user from which the encrypted data has been copied or transferred to the copyright control center, the request is accepted. If the first user information is not presented at this time, the user is recognized to be the first user and not the second.

user who has received the copy or the transfer of the encrypted data from the first user. Thus, the request for the secondary use is not accepted.

The copyright management center which acepts the request of the secondary use transmits the second crypt key for decrypting the encrypted data, the third crypt key for reencrypting and redecrypting the decrypted data and the copyright management program for the aforementioned decryption, the reencryption and redecryption, to the second user.

The outline of the copyright management system 3-33 described in the Japanese Patent Application No. 6-264199 is described as follows.

This copyright management system uses the first public-key prepared by the user, the second private-key corresponding to the first public-key the second public-key, the second private-key corresponding to the second public-key, and the first secret-key and the second secret-key prepared by the datase on base.

The database side encrypts the data which is not the encrypted by using the first secret-key, and encrypts the orbits secret-key by the first public-key, and the second secret-key by the second public-key. These encrypted adata and the encrypted first secret-key and second and second are secret-key are transmitted to users.

The user decrypts the encrypted first secret-key by using the first private-key and decrypts the encrypted data by the decrypted first secret-key for use. Then, the second private-key so that the decrypted second secret-key by the second private-key so that the decrypted second secret-key is used as a crypt-key for data storage; copy and transfer after the decryption of the data.

The outline of the data copyright management system described in the Japanese Patent Application No. 6-2-264201 is described as follows.

In the case where new data is prroduced by editing a plurality of encrypted data which are obtained from the database and is encrypted to be supplied to others, the crypt key for a plurality of data which are original materials and edit program as editing process with a digital signature are used as a use permit key.

When the user who has received the edited and encrypted data requests for use by presenting the digital signature to the copyright management center recognizes the editor on the basis of the digital signature. Only in the case where it is recognized that the editor is the authorized user of the edited data; the crypt key for use is provided to those who request for use.

The outline of a method described in the Japanese \*\*\* /
Patent Application No. 6-269959 is explained as follows: \*\*\* |

A first user receives the encrypted data in which the original data is encrypted by the first crypt key from the database and decrypts the data at the time of usage. After that, the data is encrypted by a second crypt key generated with a predetermined algorithm using one out of the first crypt key, the first user data; and the data

usage frequency or a combination thereof, and is stored, copied and transferred.

When the second user requests the secondary use:

of the data, the data copyright management center generates the second crypt key with a predetermined algorithm by using one out of the first crypt key of the original data, the first user data and the data use frequency or a combination thereof to be provided to the second user!

The second user to whom the second crypt key is a provided decrypts the encrypted original data by using 100 the second crypt key for usage.

- 3 DM Protection Fig. - このは、 のでは他には、 [Embodiment 3] ではたりやのは知识的は 2条では しゅは借いまたととは、 ・ のきらいわれて、それの時

The system shown in Fig. 4 is a crypt key system of as embodiment, a where the present invention is applied to the database system or the VOD system.

Like the crypt key system shown in Fig. 3 of embodiment 2.5 in this crypt key system; the television broads casting programs and the crypt key pass through a single 20 path which is the CATV line; however, these may pass through different path, as a matter of couse:

this system comprises a CATV station 31 for data 2 broadcasting; a data managing center 33 such as data-base, a video system or the like; a receiving apparatus # 25 34, a data communication apparatus 35 and a user terminal 38,644,645 (1994) and the communication of the like in the communication apparatus 35 and a user terminal 38,644,645 (1994) and the communication of the communication apparatus 35 and a user terminal 38,644,645 (1994) and the communication apparatus 35 and a user terminal 38,644,645 (1994) and the communication apparatus 35 and a user terminal 38,644,645 (1994) and the communication apparatus 35 and a user terminal 38,644,645 (1994) and the communication apparatus 35 and a user terminal 38,644,645 (1994) and the communication apparatus 35 and a user terminal 38,644,645 (1994) and the communication apparatus 35 and a user terminal 38,644,645 (1994) and the communication apparatus 35 and a user terminal 38,644,645 (1994) and the communication apparatus 35 and a user terminal 38,644,645 (1994) and the communication apparatus 35 and th

The data managing center 33 and the CATV station 31 are connected with a direct means for connecting with a communication line such as a dedicated line or the like. 30 or with an indirect means such as flexible disc or the like. The CATV station 31 and the receiving apparatus 34, and the CATV station 31 and the data communication apparatus 35 are connected with the CATV-line 37. Incidentally, instead of the CATV line 37, a communication line which is an appropriate data broadcasting or available for data communication can be used. The receiving apparatus 34 and the user terminal 38, and the data communication apparatus 35 and the user terminal means are connected with a direct means such as a flexible.

What is shown with a solid line is an uncrypted data path in Fig. 4 and what is shown with a broken line is an accentrypted data path as a solid line is an accentrypted data path as a solid line is an accentrypted data path as a solid line is an accentry to the solid line is an accentrate to the solid line is accentrate to th

The data is exchanged between the data managing center 33 and the CATV station 31 in principle with a dedicated line or a flexible disc. In addition, the data may be also exchanged with a communication line, a broadcasting satellite, a communication satellite and a terrestrial wave-broadcasting. In such a case, the data is encrypted.

This crypt key system adopts the secret-key cryptosystem and a public-key cryptosystem.

The data managing center 33 prepares and supplies 55 to the CATV broadcasting station 31 the public-key Kbd and the private-key Kvd common in all the data to be supplied and the secret-key Ksdi which is different from one data to another. The CATV station 31 encrypts the

received secret-key Ksdi by using the public-key Kbd of the data managing center 33

To Similar Cksdikbd=E (Kbd, Ksdi)

valable in the pro-

and broadcasts it by multiplex teletext broadcasting using scanning lines during the retrace line blanking interval of the analog television picture signal, the data broadcasting using a sub audio band of the analog television audio signal, FM multiplex broadcasting, or digital data broadcasting.

For iconvenience of the data usage, menu showing titles of available data and introduction of data outline can be also supplied without encrypted to promote the use. 49

User who selected the desired data requests by the menu or the content introduction requests for using the data to the data managing center 33 via the CATV line 37 by using the data communication line 35 through the CATV station 31. At this time, the user transmits own public-key/Kbu to the data managing center 33.

The data managing center 33 which has received the request for use from the user enctyps the data M by the secret-key-Ksdii and a managing center 33 which has received to the request for users and the secret-key-Ksdii and a managing center 33 which has received to the request for users and the secret-key-Ksdii and a managing center 33 which has received to the request for users and the secret-key-Ksdii and the secret-

reviews archegant coemproses seeks buttless

omgenoran a Cmkşdi≟E (Ksdi, M) töllerin ali dibbbli dila

The baser who receives the encrypted private-key Ckvdkbucof the data managing center decrypts there are encrypted private-key Ckvdkbu by the user private-key.

Kvu rights and the base are miles and bridges are as a second of the second of t

Kvd=D (Kvu, Ckvdkbu)

ent in percent attained by the end of the way and sind and decrypts the encrypted secret-key. Cksdikbd/by the encrypted secret-key. Cksdikbd/by the encrypted private-key. Kwd of the data managing center-way percent and end of the case are the end of the

earth of the desirable formation and the second sec

secret-key.Ksdirof the data managing center to a distance state overstone and to refer to the distance at the distance of the

we send that is a set industry of the beneath and usesit, to a fit beneath the set of the work of the beneath of the set of the set

Since the system structure of embodiment 4 is: the same as; embodiment 3 shown in Fig. 4, explanation; thereof will be omitted as:

This system adopts the secret-key cryptosystem and the public-key cryptosystem as the crypt key systemsimilarly to embodimental nembodiment 3; the private-key Kvd of the data managing center is encrypted

45

by the public-key Kbu of users who request for use while in embodiment 4, the private-key Kvd of the data managing center is distributed in advance by using the IC card or the like and stored in the user terminal. In embodiment 3 data M is distributed corresponding to the request for data usage, while in embodiment 4 the data M is broadcast by means of the CATV line or the satellite broadcasting irrespective of the request for data usage.

When the user subscribes a comprehensive contract for using the database with the data managing. 10/2
center, the private-key Kvd of the data managing center
which is commonly used with all data to be supplied is
previously distributed to users by a recording medium
such as an IC card or the like or a CATV line 37; and
stored in the semiconductor memory of the user terminal in 18.
38, the hard disc or a flexible disc.

The data managing center 33 prepares a secret-key Ksdi different for each supplying data and a public-key Kbd, and supplies them to the CATV station 31. The CATV station 31 which receives the secret-key Ksdi (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key Ksdi (by the public-key kbd (1) 20 encrypts the secret-key (

ー A **Cksdikbd=E (Kbd;iKsdi)** es Doale (コイアルタン) (A みつかないが、 avil y Avis y Avis

and broadcasts it by means of teletext multiplex broadcasting using scanning lines during the retrace blanking interval of the analog television picture signal, data broadcasting using the sub audio band of the analog television audio signal, FM multiplex data broadcasting or idigital data broadcasting.

At this time, for the convenience of the data usage, menu showing the titles of data which can be used, or a content introduction for explaining the data outline for promoting the data usage can be also supplied without encrypted.

The CATV station 31 encrypts the data Mby the secret-key Ksdi

👉 🗠 Cmksdi=E (Ksdi, M) ார் சர்வக் அரிந்த

and broadcasts it via the "CATV" line irrespective tof the prequest for use /q one if with the analysis of the beasers.

The user incorporates desired data out of the data which is broadcast via the CATV line on the basis of the white menu or the content introduction into the user terminal 1.45 by using a receiving apparatus 34.7 (1.11) and 10 (1.11) at 1.11

The user decrypts the encrypted secret-key Cksdikbd by the private-key Kvd of the data managing center which is stored in the semiconductor memory into the user terminal 38,a hard disc or a flexible disc.

Ksdi = D (Kvd, Cksdikbd)

and decrypts their encrypted data Cmksdi by the brid decrypted secret-key Ksdi (1978) and the brid as \$100.000 as \$100.0000 as \$100.0000 as \$100.0000 as \$100.0000 as \$100.0000 as \$100.0000 as \$100.0

M=D (Ksdi, Ksdikbd)

for use.

Other modifications of the embodiments for distributing the crypt key will be explained.

[Embodiment-5]

In aforementioned embodiments, the public-key Kbd of the data managing center is broadcast from the broadcasting station instead of the communication line. Thus, it is impossible to confirm whether the public-key Kbd is:

In such a case, the private-key Kvd of the data man-, aging center is used for digital signature to the public-key and case kbd of the data managing center.

Skbdkvd=E (Kvd, Kbd)

to be broadcast together with the public-key Kbd of the share data managing center.

The user recognizes the digital signature Skbdkvd" by the received public-key-Kbd of the data-managing center the control of the data-managing digital center.

The second of th

Roman Strangers of

in a search dinagra

1. CN 1.5

Kbd=D (Kbd, Skbëkvd) 🐟

and when it is justified, use the public-key. The late the public-key.

[Embodiment 6]

In embodiment 5, in the case where the data:man- start aging center adopts the membership system for preliminarily registering the use of the database, the public-key Kbui of users who are members is also preliminarily registered with the data managing center.

The data managing-center encrypts the public-key Kbd of the data managing center by the public-key:Kbuir dwg of each user

¿ Ckłodkłoui=E (Kłoui, Kłod). Wolad garabi intertracia war war za problek war spiracia.

Digital signature is made to the the public-key Kbd of the rank data managing center by using the private-key. Kvd of the rank data managing center and the public pitch invade with soft and the public pitch in a control of the rank data managing center.

Skbdkvd=E (Kvd,:Kbd):ade and add and nest

Then, the encrypted public-key Ckbdkbui different from a none user to another and the digital signature Skbdkvd and are sent to the broadcasting station to broadcast the processed encrypted public-key Ckbdkbui and the digital signature Skbdkvd.

At this time, the uncrypted user identification information of each user is broadcast by adding to the encrypted public-key Ckbdkbui if-necessary.

Uthe uer who has received the broadcast encrypted and public-key Ckbdkbui and the digital signature. Skbdkvd decrypts the encrypted public-key Ckbdkb of the data and managing center by the public-key Kvuis

Kbd=D (Kvui, Ckbdkbui)

ii: 30

Ē

and stores the decrypted public-key Kbd of the data man-. . . . . . . . 43 aging center in the user terminal.

The user recognizes the digital signature Skbdkvd by the received public-key Kbd of the data managing is at

#### Kbd=D (Kbd, Skbdkvd).

and if it is justified, uses the stored public-key Kbd of the data managing center.

In this manner, a crypt key different from one user to another can be distributed.

据点,1966年1月1日 · 1000年1月1日

#### [Embodiment 7]

Users present their own public-key Kbu to the data managing center at each time of access or request to the : - - if data managing center.

March 1987 建氯化钾 1987

The data managing center which receives the request from the user encrypts the requested data M by the public-key Kbu of the user

#### Cmkbu=E (Kbu, M)

and sends it to the broadcasting station. The broadcast- . 25 ing station broadcasts the received encrypted data Cmkbu.

The users who receives the broadcast encrypted data Cmkbu decrypts by the private-key Kvu of the user WARNED FAIT OF THE FIRE OF

general control ex

and use it.

\_ \*\* 41 T ( 1 T ) Figs.:5(a) through 5(c) show the modified examples which use the crypt key system of the present invention.

Each esample shown the structure in the figure is applied the crypt key system, in electronic market transaction using the electronic data interchange system, to the credit settlement in retail shops shown in Fig. 5 (a); the settlement by means of an electronic check shown in 40 in Fig. 5 (b); and the whole sale conducted by makers and ... the like shown in Fig. 5 (c). THE STATE OF STATE

In these systems, a digital signature is used in addition to the secret-key cryptosystem. These systems comprise a user 42, and a retail shop 43, a financial organization:44 or a sholesaler 45 such as a maker the like which is a World Wide Web (WWW) server on the internet. But only the last of a control

#### [Embodiment 8]

adie sindsah

tally demand and all

In the credit settlement in the shop shown in Fig. 5. (a), the shop 43 broadcasts a data Ms such as order form ... format, credit card format, advertisements, catalogs. previews products description, and content introduction ~.55 of a database, and menu, charge schedule and price list, via the satellite 41 and a CATV line.

User 42 who receives the data Ms such as order form format and a public-key Kbs of the shop 43 encrypts the user secret-key Ksu by the public-key Kbs of the shop 

Cksukbs=E (Kbs, Ksu)

CHANGELL TO C

end of grib

and enters Mu items such as the order content, the payment amount and a credit card number with encrypted by the secret-key Ksu of user 42 on the basis of information such as advertisement, catalog, products description and charges/prices list: after the after the action of the case.

> extraction years in the might be given by the parties. urnesador Cmuksu≃E.(Ksu,;Mu),au, yincher en in ir c

when needed, compresses Mu into a compressed document-mu and sign by digital signature by the private, and key Kvu of the user 42 2000 00 samete with space (sq. Chr. Lington in confirm of a

mission paracter of a security of the little of the

APP ARE TO A POST OF CATE OF THE PARTY.

Cabandia Bras to Chenta a a a transferance a

neilal orda brokningstrig.

and transmits it to shop 43 attached with the public-key Kbu of the user 42 via the network 47,

The shop 43 which has received the order decrypts the encrypted secret-key Cksukbs of the user 42 by the private-key Kvs of the shop 43

ეისიკან **Ksu≒D (Kvs, Cksukbs)**ც თ. და სამშეს

timber on it is also greater that the same is the table to and decrypts the encrypted order document Cmuksu by the decrypted secret-key Ksu of the user:42g-a page at a market

Mu#D:(Ksu; Gmuksu)art not arms the tw

situil litau i Amedinorini, ambito autification in territoria. Them, order, acceptance is: executed. are supplied of \$2.000 as

903.

When the digital signature Smukyu is recognized by the public-key Kbu which the user 42 attached and (in this hid promotes the children in the

mu=D (Kbu, Smukvu),

a receipt is sent to the user 42 via the network 47.

In this system, it is possible to prevent the unjustified use of the credit number because the credit card number to the entered in the order form is sent with encrypted and regular

Further, the following process enables reliable transaction: the algebra Arthur Bender 1200 and any cast back The shop 43 compresses the digital data Ms1 of the order form format, the credit card format, advertisement, ... catalog, a preview, products description, and content introductionof the database and menu/charge schedule/price list-into a compressed document mst; with diga... ital signature by the private-key Kvs of the shop 43

Smslkvs=E (Kvs, msl) = 55.1

and broadcasts it attaching the public-key Kbs of the shop 43 so that users recognizes the digital signature , Smslkvs by using the public-key kbs of the shop 43

ms'=D (Kbs, Smskvs).

Contraction.

[Embodiment 9]

In the settlement by means of electronic checks shown in Fig. 5 (b), the bank as financial organization 44 broadcasts the blank check format-Mf which is digital data attached with the public-key Kbf of the bank 44 via the satellite 41 or the CATV line. 10: 18: U.15:

The user 42 who receives the blank check format Mf encrypts the secret-key Ksu of the user 42 by the bank of public-key Kb and an analysis of the public-key Kb

> THE PROPERTY OF STREET Cksukbf=E (Kbf, Ksu), a primatot an en el

> > The resident to the letters

enters Mu items concerning a payee and the payment amount with encrypted by the secret-key Ksu of the user 42 / gg, ( ) . . . Cabbin profession in the Studential

And in with a County vastes Cmksu=E (Ksu, Mu), ...

when needed, compresses Mu to the compressed doc- 20 ument mu, and sign by digital signature by using the private-key Kvu of the user 42

de les licht lieth ville in die bei vinde als Smukyu=E<sub>i</sub>(Kvu, mu)<sub>i</sub> or in seconds that second

วาวรูกกา เหตุกรมี เพียงสลาก ราก ( ve กันที่ ) a ที่ (อยยายย **25** and transmits them attaching the public-key Kbunof the user 42 and the encrypted secret-key Cksukof of the user 42 which is encrypted by the the public-key (Kbf of the again bank 44 to the bank 44 via the network 47 mm graph and bank as

The bank 44 which receives the described check uses the bank private-key Kvf to decrypt the encrypted secret-key Cksukbf of the user 42

and broading in the are normalised and one of their

Ksu≝D (Kvf, Gksukbf),
 Normal grade of the control of

er North Chair Committee of the Chairman of th decrypts the encrypted data Cmuksu of the payee and the payment amount by the decrypted user secret-key Ksu (A) have the control of seating the con-

The will be all galaxies and entities on Mu=D (Ksu, Cmuksu)

na unit a litracida angela 9 na ayang **yasabso**ra estT and recognizes the described contents and the currency is as exchange processis/executed/ if standboard one Political gra-

Furthermore, the bank recognizes the user 42 by .... Smuksu with the digital signature using the public-key :: 45 Kbu added by the user 42

·= ::5₹:\∀:Ö

NAME GROWS NO POR

mu'=D (Kbu, Smuksu)

... in a marin chalded a

encrypts the confirmation document Ms2 by the public- 50 key Kou added by the user 42 🚓 TO NOT THE THEORY

Cms2kbu=E (Kbu, Ms2)

and send it back to the user 42 via a network 47.

The user who receives the encrypted confirmation document Cms2kbu from the bank 44 decrypts the encrypted confirmation document Cms2kbu by the private-key Kvu of the user 42

Ms2=D (Kvu, Cms2kbu)

and confirms the content.

23 13

According to the system, since the patty to which the payment is made and the payment amount are encrypted and described in the check, it is possible to prevent the unjustified use of the content described in The second of the second of the second the check.

In addition, the blank check format Mf which is digital data is xmpressed into a compressed document mrand signed by digital signature by using the private-key Kyfo ..... of the bank 44

Smfkvf=E (Kvf, mf) A COMPLETE SECTION OF THE PROPERTY OF

to be broadcast attaching the public-key Kbf of the bank beg 44. The user recognizes the digital signature Smskvs by the public-key Kbs of the bank 44

mf'=D (Kbf, Smfkvf).

The confirmation document Ms is further compressed into a compressed document ms with digital signature and by using the public-key Kbu added by the userate the control and the state of the control and the control and

nell in the first and boar

Smskbu=E (Kbu, ms)

Thus, the bank can recognize the user who has entered on the check,  $(1,1) \in \mathbb{R}^{n}$  ,  $(2,1) \in \mathbb{R}^{n}$  , and  $(2,2) \in \mathbb{R}^{n}$  , and a s blus (980) . . .

[Embodiment 10] Comment for the second secon Comments of the second

At the sholesaler 45 of a maker or the like shown in Fig. 5 (C), the wholesaler 45 forms a proforma invoice 222 format Mw1 into a compressed data mwl and sign by dig- , o. ital signature by using the private-key Kvw of the wholesaler 45 community testing the engineering of the best and

et Smwikvw=E (Kvw, mwl) + 345.0 state for a

est na liciliade e combinatore per l'estragencial parse and broadcasts it attaching the public-key Kbw of the wholesalen 45 via the satellite 41 or CATValine (1990) and a satellite (1990) and a satellite (1990) and a satellite (1990) and a satel

រក់ ខណ្ឌស្លាស់ នាមនេះ គឺមានសម្រាប់ ដែល

the control of the ball of the both statem

The user 42 Which is a shop receives the broadcast neg proforma invoice format Mwl and the public-key Kbw of the wholesaler 45, and encrypts the proforma invoice request Mu by the public-key Kbw of the wholesaler 45

> ★ Cmukbw=E (Kbw, Mú) 1 (A) 19 (Problem 2) un a la fruite de cui arai estrettet ger

and transmits it to the wholesaler 45 via the network 47. 1000

At this time; the proforma invoice request Mu is compressed to compressed data mu when needed, and that signed by the digital signature by using the private-key - :: าง รากับ แล้ว เรื่องที่ สารัสทรา ขาว ราการที่ และ พระสาร Kvu of the user 42

to be transmitted together with the public-key Kbu of the user 42 to the wholesaler 45.

∵.5'

. :

30

A SHIE!

The wholesaler 45 which receives the encrypted proforma invoice request Cmukbw decrypts the encrypted proforma invoice request Cmukbwby the private-key Kvw of the wholesaler 45

٠..

and recognizes the described proforma invoice request Mu. fangja chhair leis in h Control of the self-

Further, the whole saler 45 recognizes the digital 10 signature Smkyu by the public-key Kbu of the user 42: 4 and

. . .

200

#### mu=D (Kbu, Smkvu)

and estimates to the proforma invoice and encrypts the proforma invoice Mw2 by the public-key Kbu of the user 42 Transfer to Tay 1911 1911 1911

#### Cmw2kbu=D (Kbu, Mw2)

and then, transmit it to the user 42 via the network 47.

The user 42 who receives the encrypted proforma invoice, Cmw2kbu, from the wholesaler 45 decrypts it by the private-key Kvu of the user:42

#### Mw2=D (Kvu, Cmw2kbu).

According to this system, since the public-key and the private-key are used, there is no fear that the content of the proforma invoice is stolen to be used and also different proforma invoice can be made for each user.

In the systems shown in Figs. 5 (a) through 5 (c), since each format and advertisement with no need of secrecy-are broadcast via satellite or CATV broadcasting, the data can be effectively transmitted.

Ascexplained above, a multimedia system can be realized which combines general information media -- ? such as television broadcasting and audio broadcasting with data communication media using computers by using the crypt key system of the present invention, whhile the general information media and the data communication media has been existing so far as an independent system each as present a perfect of the second sec

A concrete structure for realizing the multimedia systam. tem will be explained as follows:

The current television broadcasting is provided by 59 means of an analog system through terrestrial wave broadcasting, satellite broadcasting or CATV broadcasting. In the meantime, most general data communication line is a public telephone line. and the state

In such a system structure, the crypt key system according to embodiment 1 shown in Fig. 2 can be used. 44 as a basic structure of a system for realizing a video-ondemand. The broadcasting station broadcasts the public-key Kbb in multiplexing with the sub audio band of an 55 audio zone in the scanning line of the vertical retrace interval of an analog television broadcasting program.

Users who wish to use the television program encrypt their own secret-key Ksu by the public-key Kbb broadcast from the broadcasting station

٠ į. v ≥4 4nad ≥ ٠:٠٠

and request for the usage by transmitting the the encrypted secret-key Cksukbb to the broadcasting staing material advistory tion via a communication line.

The broadcasting station decrypts the encrypted" and secret-key Cksukbb of the users by the private-key Kvb of the broadcasting station.

ตลทyมน ล**หรม=D (Kvb;Cksükbb)**Ж . เลือน เป็น สายต่ asu ann a mail fuil turbacha an a lèir in ma tha aibithe

scrambles the broadcasting program by the decrypted secret-key Ksu and broadcasting it.

The users descrambles the scrambled program for use by their own secret-key Ksu.

20 , By adopting such a structure persons other than users those who request to use the program cannot use \$4 '9 · · the program.

As a basic structure of a system for realizing the video on demand and pay-per-view in such a system structure, the crypt key system shown in embodiment 4 or embodiment 54h Fig. 4 can be used 3 100 ff 110 200 110

The broadcasting station 31 encrypts by the secret: "" key Ksb of the broadcasting station 31 the bublic-key Kbb of the broadcasting station 31% and and and a second and fire bear age with the letter age used her check

betq or Cksbkbb≆E (Kbb, Ksb)efe mo Hosdwert of the well and to to to to got a tree

and broadcasts it via the communication line 37 in multiplexing with the scanfilng line or a sub-audio band of the retrace interval of the analog television broadcasting programa. A Tarris to A Terris (a) and the

User 38 who wishes to use the television program? 38 requests for the usage by transmitting own public-key Kbu to the broadcasting station 31 via the communicaingustation of the control of tion line 37.

The broadcasting station 31 scrambles the broadcasting program by the secret-key NSD of the broadcast-11 PE ing station and broadcasts it via the communication line 7 12 37. At this time, the private-key Kvb of the broadcasting station 31 is encrypted by the public-key Kbu of user 38

经主义 化硫二氯二甲烷

to a different control of

Ckvbkbu=E (Kbu, Kvb) . 1

and is broadcast via the communication line 37.

The user 38 decrypts the encrypted private key 1714 Ckvbkbu of the broadcasting station and the control of the c 31 by own private-key Kvu

Kvb=D (Kvu, Ckvbkbu),

decrypts the encrypted secret-key Cksbkbb of the broadcasting station 31 by the private-key Kvb of the decrypted 8. L. L. S. J. C. 1993 9 7 7 7 broadcasting station 31

50

1. 1. 3

M. 127

#### ...Ksb=D (Kvb, Cksbkbb)

and descrambles the scrambled broadcasting programby the decrypted secret-key Ksb of the broadcasting station 31.

By adopting such: a structure, persons other: than users who request to use the program cannot use them.

Further, the crypt key system can be applied to television shopping which is frequently conducted currently by combining the television broadcasting and the television broadcasting and the television broadcasting and the television broadcasting and the stelevision broadcasting and the stelevision

In the currently conducted television shopping which uses the analog television broadcasting, product introduction and sales method are presented on the television screen so that users record information on the sales method manually and request for the purchase thereof by a telephone on the basis of the recorded information.

On the contrary, the crypt-key system according to the present invention proposes a transmission of data of the order format and the check format in multiplexing with the scanning line of the vertical retrace interval or the sub audio band of the audio zone.

In the meantime, an apparatus called personal computer television set which integrates the personal computer and the television set or an apparatus which combines a video capture device which is realized as an IC card, a PC card or an insertion board and a personal computer allows incorporation of the television picture.

With the combination of the multiplex data such as an order format and a check format with a video capture device, an electronic television shopping can be conducted.

In such a television shopping, when the television shopping product introduction display is broadcast; the order format and the check format are broadcast in data multiplex with the scanning line of the vertical retrace linterval or the sub audio band of the audio zone.

If the users operate the apparatus when the product introduction display of the desired product to purchase is broadcast, the order format and the check format data are incorporated with the static display picture, the control incorporated with the static display picture.

Users, who wish to use the selevision shapping enters necessary items on the order formation check format to request for the purchase. To secure the safety of the transaction at this time, encryption by the public-key cryptsosystem or the secret-key cryptosystem and digital signature are used with the system caccording to embodiments 1 to 5:

At this time, the content of transaction can be confirmed, when the purchase order is requested by adding the static display picture of the product introduction together with the order and the check.

As a simple method, the order form format, and the check format may be also transmitted as a television picture so that necessary items are entered on the order format and the check format which are incorporated as a static display picture.

15 131 . 5

In addition, the order form format and the check format can be transmitted via facsimile broadcasting which is multiplexed with the sub audio band of the audio zone.

By adopting such a method, an electronic market using electronic data intercahnge (EDI) by means of a current analog television method can be realized with the television shopping.

These video-on-demand system and the pay-perview system can be applied to the digital television broadcasting other than the analog television broadcasting.

In the case where a CATV line is used as a communication line, both the broadcasting and data communication can be carried out with the CATV line only.

Further, these video-on-demand system and payper-view system can be also applicable to transmission of high-quality audio data and moving picture data performed in computer communication networks system using low-speed public telephone line or high-speed integrated services digital network (ISDN) or in internet system connecting a plurality of computer communication network.

As an apparatus to be used, the receiving apparatus and the communication apparatus can be incorporated in the television set. Apparatuses can be also constituted as a separate apparatus by using a set top box or the like.

In addition, a constitution an apparatus referred to as a personal computer television set which is gradually prevalent or by combining a video capture device which is realized as an IC card a PC card or an insertion board for transmitting a television signal to the personal computer can be used.

Richard Lander Biller Begen, in Burgerte

#### Claims,

35

the first of any of the same and Crypt key system comprising a broadcasting station (1), a database (2), a receiving apparatus (4), a data communication apparatus (5) and a user terminal (8); wherein the company of the second secon said database (2):and said broadcasting station:(1) are connected with an online communication means such as a dedicated line; or the like on a off-line means such as a flexible disc or the like; bine :(78) said database (2) and said data communication apparatus (5) are connected with a communication 7 10 10 10 10 10 Ins 18 17400 said broadcasting station (1) and said receiving apparatus (4) are connected with a radio wave (6); whereas between said receiving apparatus (4) and said user terminal (8) and between said data communication apparatus (5) and said user/terminal (8) said are connected with direct online means or with off-line means such as a flexible disc; also a last? said database (2) prepares a public-key and a private-key and supplies said public-key to said broadcasting station (1); the last term and the bounds said broadcasting station (1) broadcasts said received public-key; said receiving apparatus (4) transmits said received

120

ratus (34) and between said CATV station and said

public-key to said user terminal (8); said user terminal (8) stores said transmitted public-. a user encrypts:a secret-key of the user by said received public-key and transmits said secret-key at 115 the time of request for the use of data which he desires, to said database (2); said database (2) which has received the request for data use decrypts said secret-key of said user by said private-key and encrypts the data by said. 10 decrypted secret-key of said user to transmit the data to said data communication apparatus (5) via said communication line (7); and the first section of said user transmits the received data to said user terminal (8) to decrypt said data by said secret-key. AGAZ & Carb ribas THE RESERVE TO SERVE

2. Crypt key system according to claim 1 wherein a digital signature of said database (2) is provided on said public-key:

3. Grypt key system comprising a CATV station (31);

- a charging center, a receiving apparatus (34); a data communication apparatus (35), and a user terminal (38), wherein: between said CATV station (31) and said receiving: 125 apparatus (34) and between said CATV station (31) and said data communication apparatus (35) are connected with a CATV line (37) 1. 30 1.300 0 between said receiving apparatus (34) and said user 19 3 terminal (38) and between said data communication 30 apparatus (35) and said user terminal (38) are connected with direct online means or with off-line means such as a flexible disc or the like; a user preliminarily registers a public-key of said 💨 user with said CATV station (31) or presents said public-key of said user at the time of request for uságe; 41% (1986) (2003) 48 (5) (8) said CATV station (31) encrypts a secret-key which is a use permit key of said CATV (31) station by using said public-key of said user who has requested the usage and also encrypts a television program by said secret-key, to broadcast both via said CATV line (37); and restlicitly a nation-valuable seem uses said user receives said encrypted television program and said secret-key with said receiving-apparatus (34) and decrypts said secret-key by a privatekey corresponding to said public-key for decrypting
- 4. Crypt key system comprising a CATV station (31), a data managing center (33), a receiving apparatus (34), a data communication apparatus (35) and a user terminal (38), wherein said CATV station (31) and said data managing center (33) are connected with online communication means such as a dedicated line or the like, or off-line means such as a flexible disc or the like; a between said CATV station and said receiving appara

said television program by said decrypted secret-

'key.'

data communication apparatus (35) are connected with a GATV line (37); between said receiving apparatus (34);and said user terminal (38) and between said data communication apparatus (35) and said user terminal (38) are connected - with direct online means or with off-line means such as a flexible disc or the like; said:data:managing center (33) supplies a publickey; and a secret-key which is a use permit key for each data to be supplied, to said CATV station (31); said GATV station (31) encrypts said secret-key for each: databby said::public-key: of rdata; managing 10:15 center (83) to broadcast; and control to toller 20 and of the a eser requests for the use of data by using said data 😘 communication apparatus (35) to said data managing center (EE) via said CATV line (37) together with transmitting a public-key of said user; 1971 - 4 . . . . said data managing center (33) encrypts the data by: 1915 said secret-key for each data; and encrypts said public-key of data managing center (33) by said public-key of said user and transmits encrypted data and encrypted said public-key of data managing center (33) together with a private-key of said data manag-> - 4 ing/center.(33):to said userya how we have the said user decrypts said encrypted public-key of data managing center (33) by a private-key of said user,

1.18%

· FEJEZ

· CONTRACTOR

長された法

M11.34

\*- 强~·==

30

5. Ohypt key system according to claim 4 wherein a digital signature of said data managing center (33) is provided on said public-key of data managing center (38) where it is strong a signature of the said public key of data managing center (38) where it is strong as a signature of the said and a said a sai

decrypts said encrypted secret-key for each data by

(33) and decrypts: encrypted data by decrypted said : :

secret-key for each data. A standar on oncome is an adven-

decrypted said public-key of data managing center

Crypt key system comprising a CATV station (31), a data managing center (33), a receiving apparatus (34), /ardata: communication: apparatus (35),- and a 🔠 user terminal (38), wherein the அம். have been a second a ca arpublic-key/of wisser is registered with said data managing center (33) in advance (131 (1382) (28.00 (13) 13 said data managing center (33) encrypts a public- "" key of said data managing center (33) by said publickey of each user to provide a digital signature on said public-key of data-managing center (33) by a private-said encrypted public-key of said data managing center (33) and said digital signature of data managing center (33) are sent to said CATV station (31); said CATV station (31) broadcasts said received encrypted public-key of data managing center (33) and said digital signature; -.. . said user decrypts said received encrypted publickey of data managing center (33) by said public-key said decrypted public-key of data control center.

50

30

45

- Crypt key system according to daim 6 wherein uncrypted user identification information of each user is further added to the encrypted public-key of said data managing center (33) to be broadcast.
- 8. Crypt key system comprising a CATV station (31), a data managing center (33), a receiving apparatus (4), a data communication apparatus (35), and a user terminal (38), wherein a user presents a public-key of said user to said data 10 managing center (33) upon requesting use of the data to said data managing center (33); said data managing center (33) receives the request for data use from said user and encrypts the data requested by said public-key of said user to send to said CATV station (31); said CATV station (31) broadcasts said received encrypted data; and said user who receives said broadcast encrypted data decrypts said encrypted data by a private-key of said user.

55

enviolent 10 10 24 10 <del>10 44</del>0 11 2000 2

5 (18) not see

## FIG.

Continuence of the continuence o

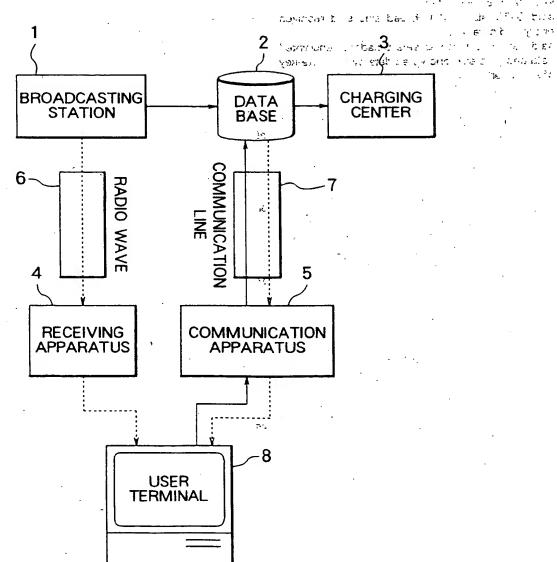
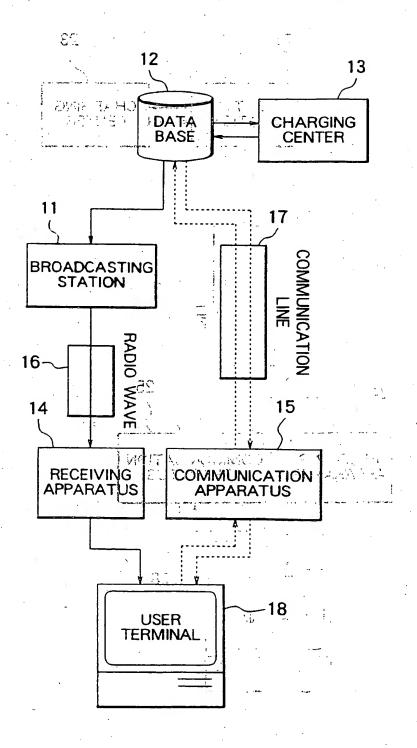


FIG. 2



# FIG. 3

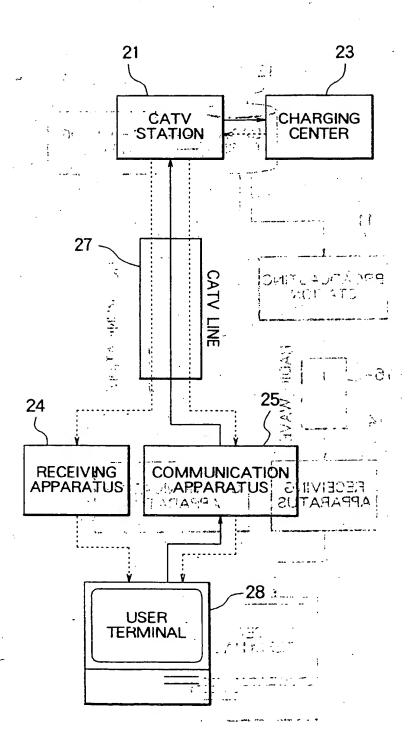
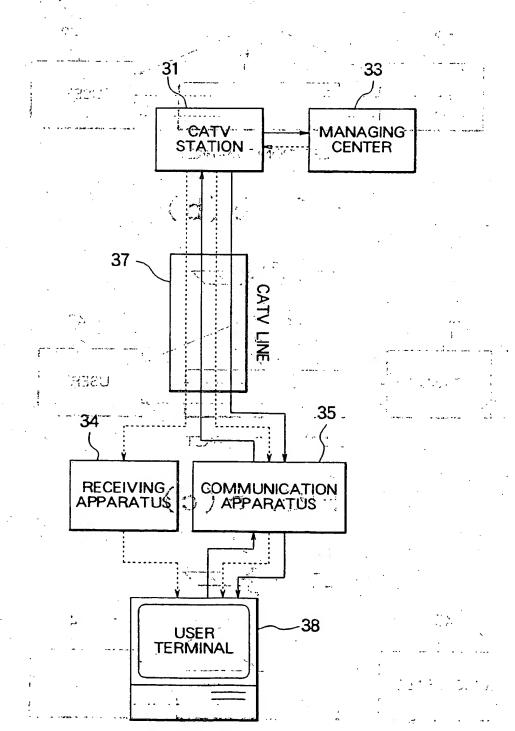
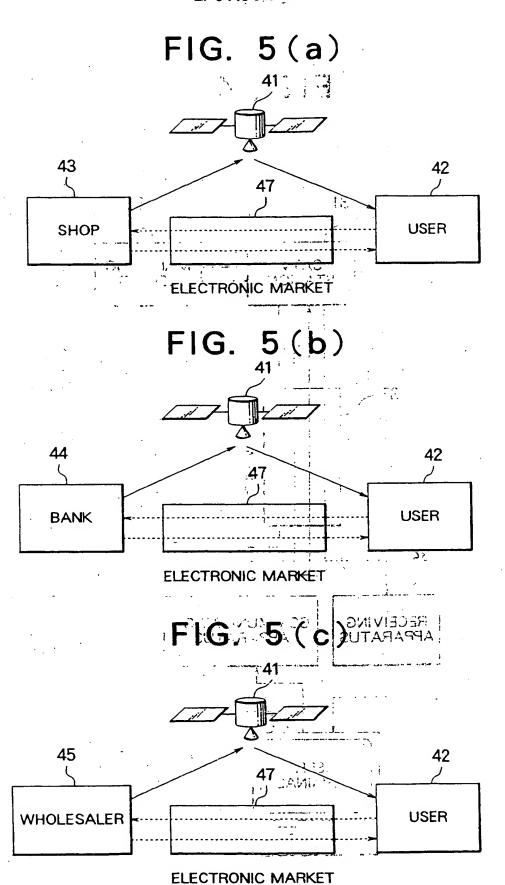


FIG. 4

(2) 3



TI BANGET IN



a a**ac**eas at attack in

(3)

18.4. 4. 19 KO 1

## THIS PAGE BLANK (USPTO)

an morati local (PS)

Jan 136 186

TO good to are Q (CS)

(84) Pes grand C. in 11 grands (48) De RR GE

Similar originations.
(Signature or origination)

P. Determine the definition of the control of the C

(90) LI HIMA 807 II

द्राप्ता का वार्षा का भागा भागा है।

TO BE ONE OF THE STORY (FT).

Character of the second of t

The control of the co

The part of the provided to the provided to the part of the part o

OM TOTAL STATE OF THE PARTY OF

F 13. 2

and the state of



**Europäisches Patentamt** 

**European Patent Office** 

Office européen des brevets



EP 0 719 045 A3

(12)

#### **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3: 16.10.1996 Bulletin 1996/42

(51) Int. Cl.6: H04N 7/167

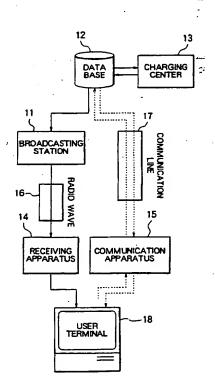
(11)

- (43) Date of publication A2: 26.06.1996 Bulletin 1996/26
- (21) Application number: 95119605.4
- (22) Date of filing: 13.12.1995
- (84) Designated Contracting States:
  DE FR GB
- (30) Priority: 13.12.1994 JP 309292/94
- (71) Applicant: MITSUBISHI CORPORATION Chiyoda-ku Tokyo 100 (JP)
- (72) Inventor: Saito, Makato Tama-shi, Tokyo (JP)
- (74) Representative: Neidl-Stippler, Cornelia, Dr. Rauchstrasse 2 81679 München (DE)

#### (54) Crypt key system for broadcast programmes

The invention relates to a crypt key system applicable to a television system, a database system or an electronic commercial transaction system or the like. This system consists of a broadcasting station 11, a database 12, a receiving apparatus 14, a data communication apparatus 15 and a user terminal 18. As a crypt key system, a secret-key cryptosystem, a public-key cryptosystem, and a digital signature system are used. The keys used in the system are either encrypted or remain uncrypted to be supplied by broadcasting. The present invention is effective in the prevention of an unjustified use of the database system, managing copyrights, and in a pay-per-view system and a video-ondemand system. Further, the present invention is effective in realizing an electronic market which uses an electronic data information system.

FIG. 2





#### EUROPEAN SEARCH REPORT

Application Number EP 95 11 9605

- 1	DOCUMENTS CONSIDERED TO BE RELEVANT  Citation of document with indication, where appropriate, Relevant					<b>7</b> (10)
	ategory		with indication, where appropriate, ant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.CL6)	
	<b>K</b> 11 11	EP-A-0 438 154	(CANON KK) 24 July 1991	1-8	H04N7/167	,
	1 4. 11	* page 3. colum	n 3. line 3 - line 31 *	3.27	1 2 2 2 2 2 2 3 3	
·	رونات. اس	* page 4, colum	n 5, line 49 - page 8,		1	
	اد ا	column 13, line	n 5; line 49 - page 8,	.]	1 1 P	1,5 -
		* figures 1-5 *				
	An in					1
22 L	S 14 2	September 1992	(SCIENTIFÍC ATLANTA) 30	1-8	De la companya della companya de la companya della	1
	,	* page I, line	5 - 1 ine 16 *	.] ,:	White grant is	1
	1771.01	* name & line	01 - nade (12.0 line 2:★	1.	And the street	
1 - 1 -	1.55	* page 14: line	41 - page 13, line 2 * 55 - page 16, line 45 *	1 .		
- "	.4.	* figures 7-10,	120***************	1		
	(ب	a Maring Heri				1 .
1	<b>4</b> :		NS, MONTREUX, JUNE 10 - 15,	1-8	· ·	1
	ડા રખ્	1993 <sup>1</sup> , 41 7 1	•			
		no. SYMP. 18,	11 June 1993,	ļ	337.	ļ., "
	4 5		ES ET TELEGRAPHES SUISSES,			
. '1	***	pages' 761-769,				• • • • • • • • • • • • • • • • • • • •
			A DEVICE FOR REAL-TIME ACCESS CONDITIONS IN A			
	່າາອາຕ	DOMAC / DACKET F	UDOCHURT CECUAL THE .		TECHNICAL FIELDS	-
	·"·	TRANSCONTROLLER		1 '	SEARCHED (Int.CL6)	
177	v - + ,		ument . * The case of the		HO4N	
, 17 J. 15	5 211	of a manager	N. 1. T. T. 1.385 (11)		* * * * * * * * * * * * * * * * * * * *	
1 11/00	A 🤼 📑	EP-A-0 450 841	(GTE LABORATORIES INC) 9	1-8	1. 6. 5. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.	1
: 1 .	٠. ٠	October 1991:				
(1)		* page 3, colum	n 1, line 56 - page 5,			1
20		column 6, line * figures 1,2 *	<b>50</b> m (144 143 144 144 144 144 144 144 144 144			c .
-		rigures 1,2	· · · · · · · · · · · · · · · · · · ·			
	•	• • • • • • • • • • • • • • • • • • • •	Trapic	! .'		
·* : '		te i i	The state of the s		Contract of the contract of th	100
\$ 25 at 32 4.	andra.	gardina i storye i di	the state of the s		And a grown to	
colai /s	id ler	On the terrest	enter tage protectes specific to		enisting macunes to g	
	V 11 11 11	मेर बाह्य हर १३४	it annemos virtos a la la virta.		ំ ប្រទេសកានុក្រភព ស្ន	
	, 1,	, a	Authorities a spirities of a			
:			THE BELL ALL THE FAME.		T 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	. :
	. :		इत्तेवध्या क्षेत्र वर्णकः	1	1 1 1 1 2 2 2 2 2 2 2 2 2 2	
• • •		: -	মন্ত্ৰ কৰ্মা ুৰ			١٠
		3 37 3	The section of the se			20
		<u> </u>		Ŧ´	1 10 10 10 10	3
	4 416 5 <u>* 1 5 5</u> 5	The present search repor	t has been drawn up for all claims			
·	1 14	Place of search	Date of completion of the search		Exemiser	1
i borco		THE HAGUE	26 August 1996	Va	n der Zaal, R	. 8.
200		CATEGORY OF CITED DO	E : earlier patent de	ple underlying to ocument, but pu	hlished on, or	1
8	X: pini Y: pan	ticularly relevant if taken alor ticularly relevant if combined	se after the filing	date:		1- 1
₹`	doc	nument of the same category	L: document cited	for other reason	S	
		n-written disclosure			ily, corresponding	1

Life the art of grants.

# This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

□ BLACK BORDERS
□ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
□ FADED TEXT OR DRAWING
□ SKEWED/SLANTED IMAGES
□ COLOR OR BLACK AND WHITE PHOTOGRAPHS
□ GRAY SCALE DOCUMENTS
□ GRAY SCALE DOCUMENTS
□ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
□ OTHER:

### IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)